Volume 1

CHAPTER 6

Communication Systems

Communications-Based Train Control
A Comprehensive Guide for US Transit Professionals
Francisco Wang

Chapter Overview

- Communication is the nervous system of CBTC — continuous, bidirectional wireless exchanges between trains and wayside
- Explore the radio technologies powering CBTC: Wi-Fi, FHSS, and emerging LTE/5G solutions
- Understand network architecture: fiber backbone, access-layer radio, and multi-layer redundancy
- Examine cybersecurity threats and defense-in-depth strategies for safety-critical networks
- Review legacy alternatives (inductive loop, leaky feeder) and communication loss response procedures

6.1

Radio Communication Technologies

Wi-Fi: The Dominant CBTC Radio Technology

- IEEE 802.11 family dominates CBTC radio deployments worldwide — mature, COTS equipment, license-free ISM bands
- 802.11n (Wi-Fi 4): Both 2.4 & 5 GHz, up to 600 Mbps with MIMO — used on NYC MTA L Line
- 802.11ac (Wi-Fi 5): 5 GHz only, up to 1.3 Gbps — increasingly specified for new deployments
- CBTC data requirements are modest: 5–50 kbps per train for position reports and control commands
- Typical AP spacing: 150–250 m in tunnels, 300–500 m elevated, with 30–50% overlap for seamless handover

2.4 GHz vs. 5 GHz Trade-offs

- 2.4 GHz: Superior range and penetration through tunnel steel and concrete
- Only 3 non-overlapping channels in North America
- Highly congested — shared with Bluetooth, passenger Wi-Fi, microwaves
- Used as backup channel in many modern systems

- 5 GHz: Higher path loss but dozens of non-overlapping channels
- Less interference from passenger devices — critical advantage in modern stations
- Primary CBTC control channel in most new deployments
- Modern hybrid approach: 5 GHz primary + 2.4 GHz backup

FHSS vs. Wi-Fi for CBTC

Characteristic	FHSS (Proprietary)	Wi-Fi (IEEE 802.11)
Spectrum	Licensed (450, 900 MHz)	ISM (2.4, 5 GHz unlicensed)
Interference resilience	Very high	Moderate
Cost	Higher (licensing + proprietary)	Lower (COTS equipment)
Data rate	100s of kbps	Mbps–Gbps range
Deployment timeline	Longer (FCC coordination)	Shorter (license-free)

CBTC Radio Communication Architecture

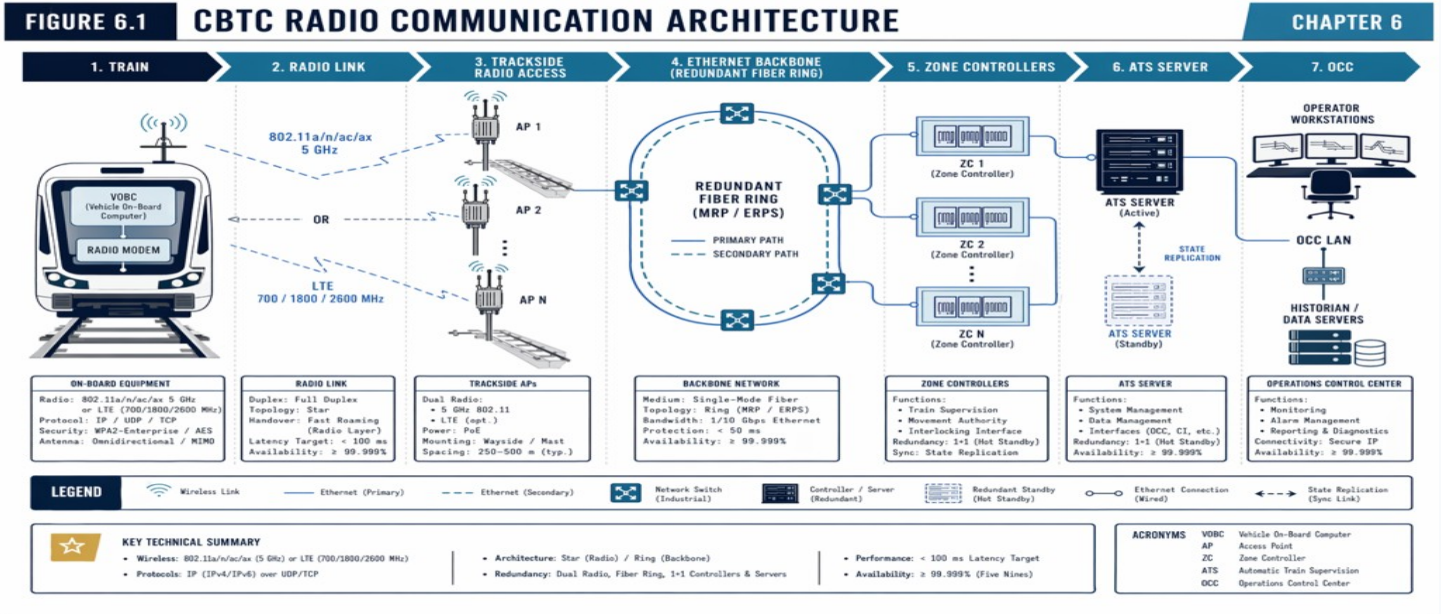

Figure 6.1 — Radio architecture showing train-to-wayside communication via Wi-Fi access points.

6.2

Network Architecture and Redundancy

Backbone Network: Self-Healing Fiber Ring

- Standard architecture: dual self-healing fiber-optic ring with automatic protection switching
- Single cable break reroutes traffic through the opposite ring direction within milliseconds
- Target availability: 99.999% (≤ 5.26 minutes downtime/year) for safety-critical paths
- Redundancy protocols: RSTP (1–5 sec recovery) or PRP/HSR (zero-switchover, 15–30% cost premium)
- VLAN segmentation isolates CBTC traffic from surveillance, passenger Wi-Fi, and maintenance data

Network Availability Targets

99.999%

Safety-critical communication availability

<250 ms

Handover deadline for seamless roaming

50K+ hrs

MTBF target for critical components

Roaming and Multi-Layer Redundancy

- Handover must complete in <250 ms — the safety-critical deadline before emergency braking triggers
- IEEE 802.11r fast roaming: pre-authentication, key caching, faster beacons → 50–150 ms handover
- Dual-radio onboard: both radios maintain concurrent Zone Controller connections via different APs
- Dual-radio cost: ~$15K–$30K per train, but eliminates single-point-of-failure risk
- Distributed Zone Controllers provide geographic redundancy against site-specific failures

Trackside Wireless Coverage and Handover

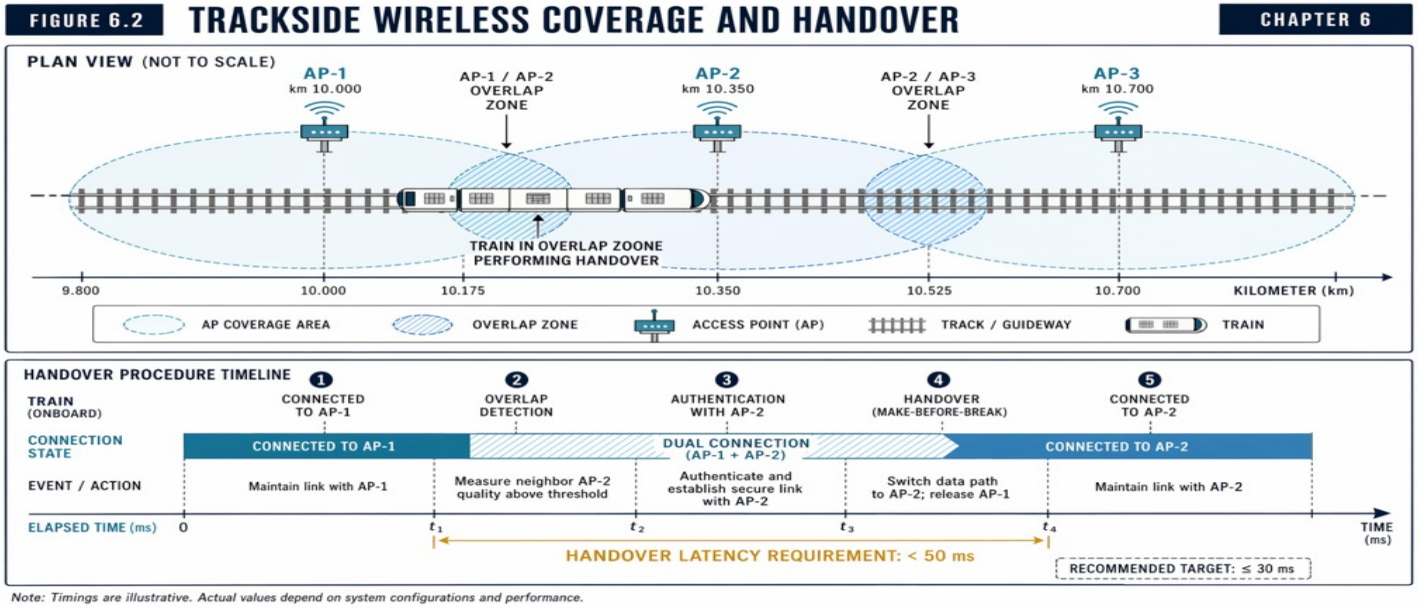

Figure 6.2 — Overlapping AP coverage zones ensure seamless train communication during movement.

6.3

Cybersecurity for CBTC Networks

The CBTC Threat Landscape

- Wireless links are inherently exposed — any attacker within radio range can attempt interception
- Key threats: eavesdropping, radio jamming, spoofing (false data injection), man-in-the-middle, DoS
- Supply chain and insider threats: compromised firmware, backdoored software, disgruntled personnel
- 2015: IOActive demonstrated remote control of European CBTC in lab — feasibility proven
- 2021: Colonial Pipeline attack prompted TSA security directives for rail/transit sectors

Defense-in-Depth Strategy

- Physical security: locked facilities, tamper-proof enclosures, monitored cable runs
- Network segmentation: IT/OT separation, air-gapping, DMZ for remote access
- Encryption: WPA2/WPA3 for radio links, TLS/IPsec for backbone traffic
- Authentication: PKI with certificate-based mutual auth, key rotation

- IEC 62443: Security levels 1–4 for industrial control systems
- NIST CSF: Identify → Protect → Detect → Respond → Recover
- TSA Security Directives: mandatory cybersecurity plans since 2022
- Penetration testing and radio security testing before deployment

Cybersecurity Defense-in-Depth for CBTC

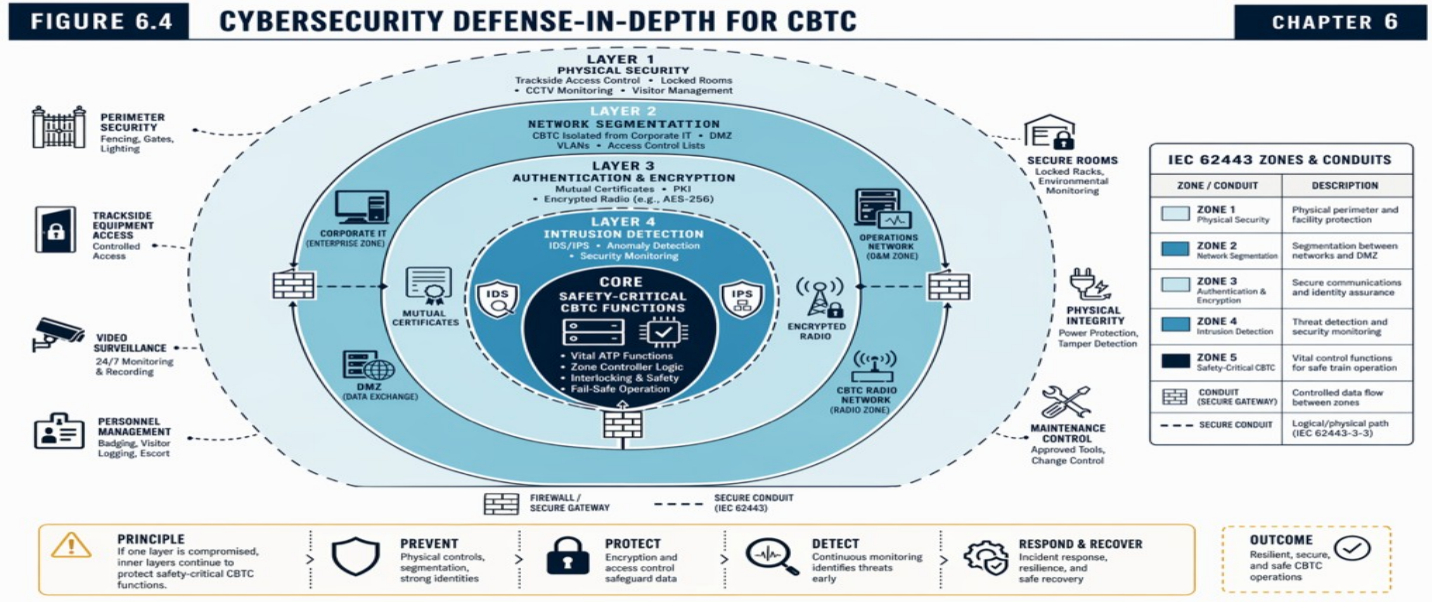

Figure 6.4 — Multiple overlapping security layers protect CBTC from physical to application level.

6.4

Legacy Alternatives: Leaky Feeder and Inductive Loop

Legacy Communication Technologies

- Inductive Loop: electromagnetic coupling at 10–100 kHz, 1,200–9,600 bps
- Short range (10–50 m per loop), dense installation required
- Immune to RF interference; no line-of-sight needed
- Now essentially obsolete for new deployments

- Leaky Feeder: slotted coaxial cable radiates RF along its length
- 19,200–115,200 bps in UHF bands (200–900 MHz)
- Uniform tunnel coverage, no handover complexity
- Repeaters every 350–500 m add cost and failure points

6.5

Communication Loss: Detection and Response

Detecting Communication Loss

- Position report heartbeat: trains transmit every 1–3 sec; loss alarm at 3–6 sec timeout
- Watchdog timers on both VOBC and Zone Controller count down with each valid message
- RSSI monitoring: Strong (>−80 dBm), Weak (−80 to −95), Critical (<−95 dBm — loss imminent)
- Timeout trade-off: too short → false alarms; too long → trains travel with stale authority
- Typical target: 3–5 second timeout balances safety and operational continuity

Communication Loss and Fallback Logic

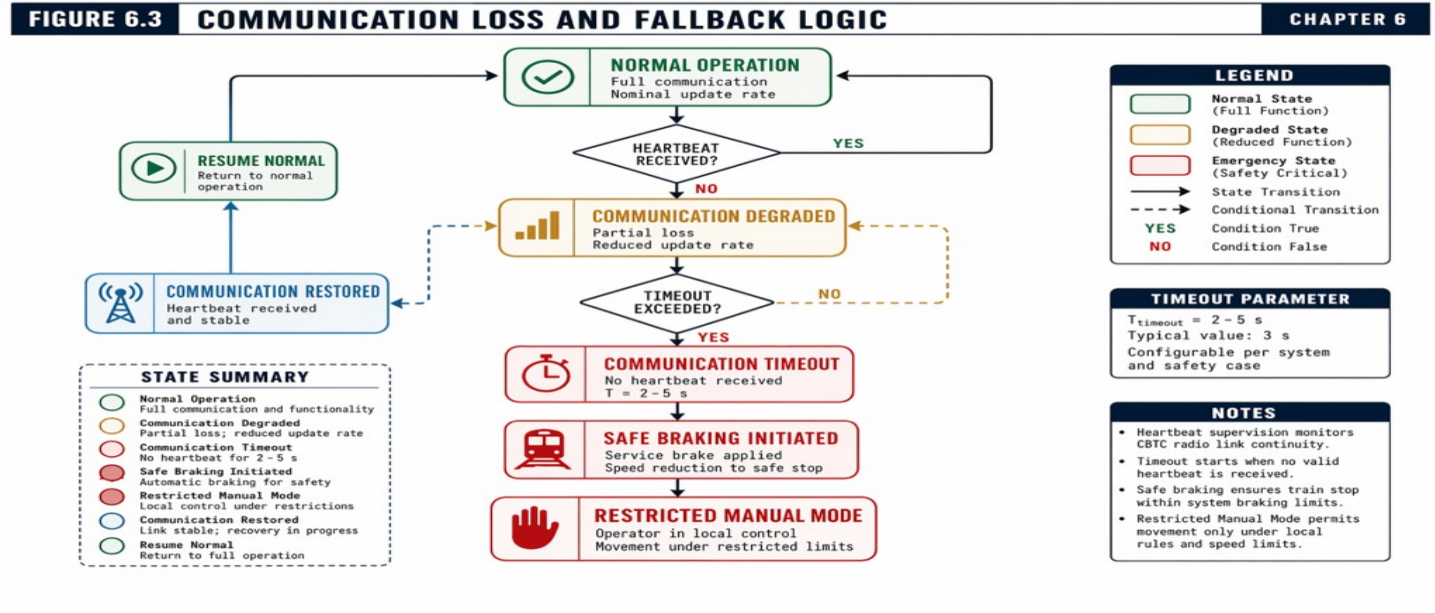

Figure 6.3 — Graduated response from degraded communication through complete loss to safe stop.

Vendor Communication Loss Parameters

Vendor/System	Timeout (sec)	Detection Method	Response
Siemens Trainguard MT	3–5	Missed heartbeat	SB + speed restriction
Alstom SelTrac	3–4	Sequence error	SB + MA revocation
Bombardier CITYFLO	4–5	Watchdog expiration	EB + safe stop
GE Adversario	3–6	Multi-layer watchdog	Adaptive per mode

Key Takeaways

1. Wi-Fi (IEEE 802.11n/ac) dominates CBTC radio with license-free ISM spectrum, COTS equipment, and modest 5–50 kbps per-train data needs
1. Dual-ring fiber backbone with PRP/HSR redundancy achieves 99.999% availability — meeting SIL 3/4 requirements
1. Cybersecurity is a safety-critical discipline: defense-in-depth with encryption, authentication, segmentation, and TSA compliance is mandatory
1. Communication loss detection via heartbeats and watchdog timers triggers graduated response within 3–5 seconds
1. Legacy technologies (inductive loop, leaky feeder) are being replaced but remain in service at several US properties

End of Chapter 6

Next: **Chapter 7: Central System — ATS and Operations Control**

Questions & Discussion